Fermilab U.S. DEPARTMENT OF ENERGY | Office of Science

Security basics for scientists (*and for anyone using the scientific tools*)

Jeny Teheran

Computer Security Awareness Day 2018

13 June 2018

Cybersecurity starts with you!

Common misconceptions

- *"Security should be left to specialists in IT".*
- *"Security is a technical problem that is hard to understand".*

Security Awareness

- Security is an ongoing process.
- The environment is constantly changing.
- You must prepare - recognize - respond.

Security is everyone's responsibility

Why your help is needed?

Because YOU are the target!

- Attackers want:
  - Your personal information (identity).
  - Your network connection.
  - Your access (privileges) to the computing resources.

Your role in cybersecurity

- You are the last line of defense!
- The majority of security incidents involve improper credential management.

" WHEN IT COMES DOWN TO IT, JIM, SECURITY IS A PERSONAL RESPONSIBILITY."

http://www.jklossner.com/

Agenda

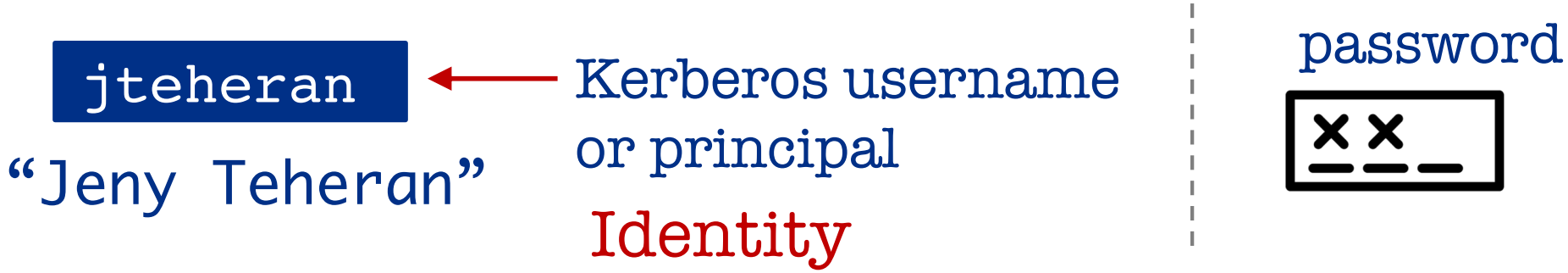
Security basics

- What is a…?
- What can you do with a…?
- How do you get a…?
- Best practices for….

i. Kerberos ticket
ii. Certificate
iii. Proxy

What is a Kerberos ticket?

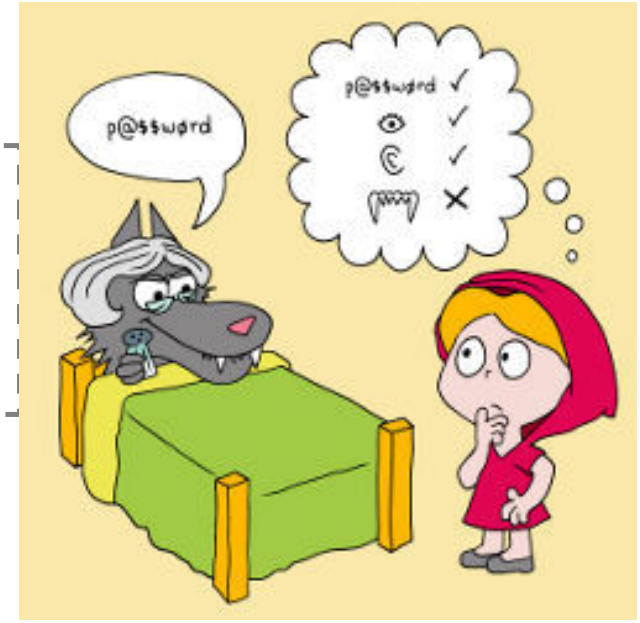
- It is a temporary identification token given to a user.
- It is similar to your driver license, it confirms who you are.
- FNAL users possess a Kerberos username & password (AKA Kerberos credentials).



Authentication

- It is the process where the identity of a subject (a user, a machine, a service, etc.) is confirmed.

Who are you?

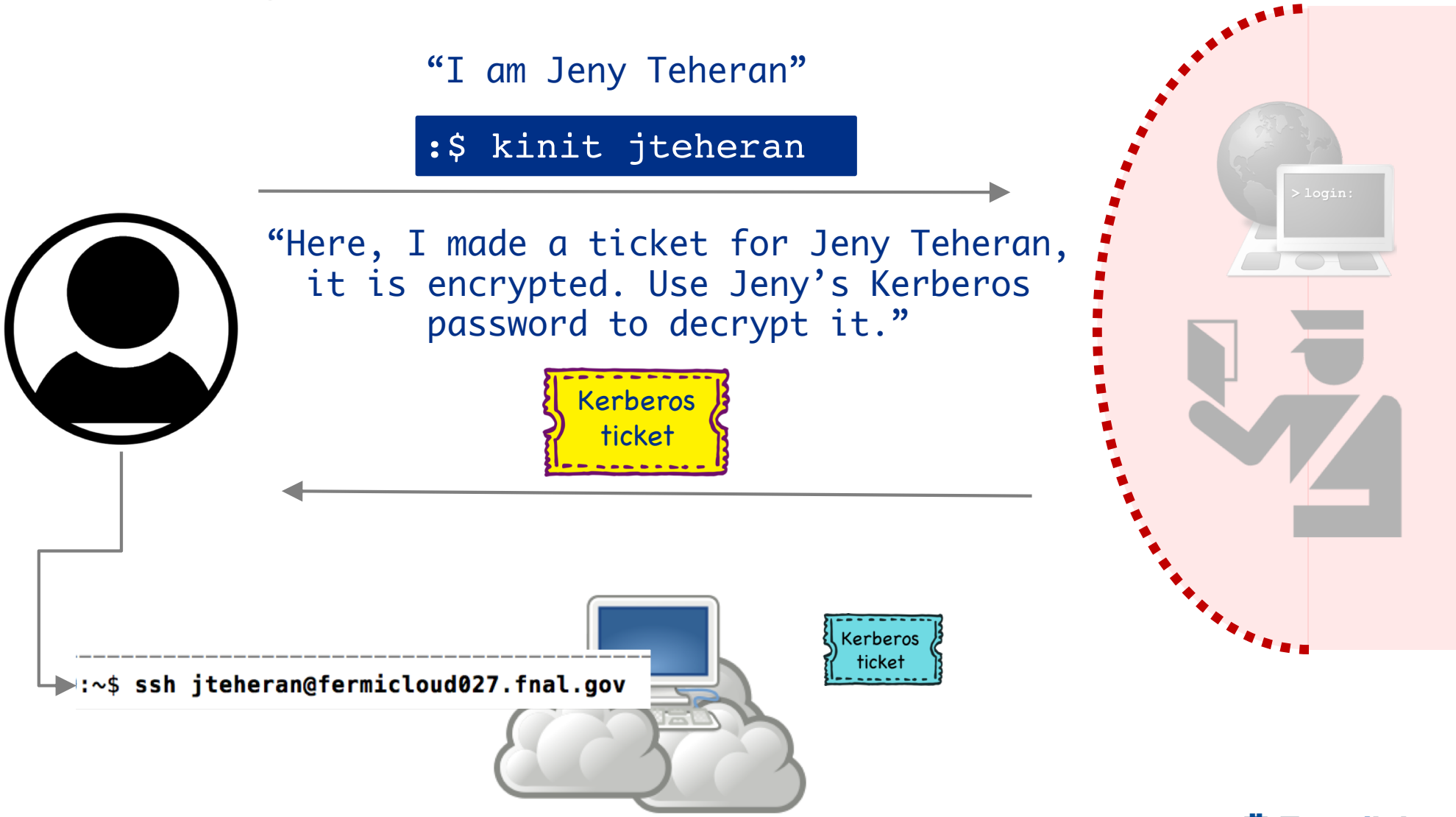


What can you do with a Kerberos ticket?

- You can prove your identity before using computing resources:
  - To SSH into FNAL interactive nodes.
- You can generate certificates

How do you get a Kerberos ticket?

- By running the command `kinit` in your machine.



Best practices for Kerberos credentials

- Choose a complex password.
- Do not share your Kerberos password with anyone.
  - It is a violation of Fermilab Security Policy.
  - You must not allow anyone else to know or use your Kerberos password.
- Never write/store/publish your Kerberos password:
  - In a .txt file.
  - In your code.
  - In a post it.

What is a certificate?

- File written in a standard format: [X.509] which confirms a subject's identity (a user, a machine, a service, etc.)
  - X.509 certificate

- It acts like an online ID card that you can carry around to:
  - Generate proxies.
  - Access web services in your browser, such as DocDb.

- It is issued by a trusted third party: Certificate Authority.

What can you do with a certificate?

- You can generate a proxy to submit jobs or initiate data transfers.
  - When generating a proxy, you should provide your certificate's passphrase.
- You can access some web services with certificate-based authentication.

How do you get a certificate?

Through the command line, running the `kx509` command

```
:$ kinit
```

Kerberos ticket — valid for 26 hours

```
:$ kx509
```

creates an [X.509] certificate based on your Kerberos ticket.

valid for 1 week

valid for 13 months

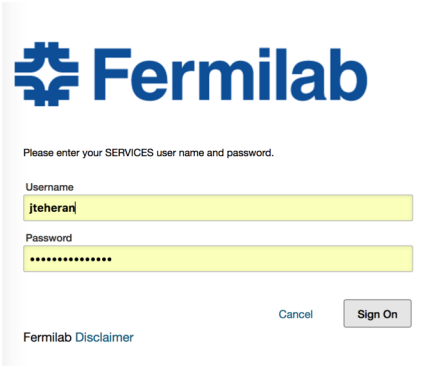
Through the CILogon website at

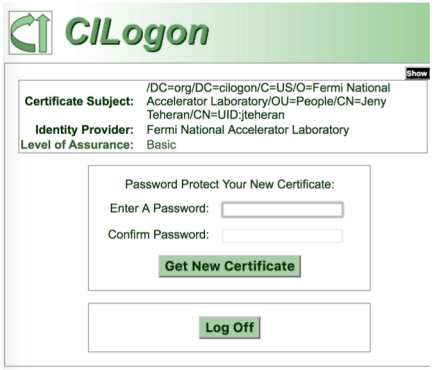
a. Go to https://cilogon.org/

b. Select "*Fermi National Accelerator Laboratory*" as Identity Provider.

c. Provide your SERVICES account and password.

d. Pick a passphrase and download the certificate.





How a certificate is different from a Kerberos ticket?

- Both are ways of representing a subject's identity.
- A Kerberos ticket lifetime is shorter than a certificate lifetime.
- You can use your certificate to prove your identity almost everywhere (in the global grid infrastructure).
- Your Kerberos ticket is only valid within a specific realm: FNAL.GOV.

Best practices for certificates

- CILogon provides you a certificate file (.pem or .p12) which contains your certificate and a secret piece of information called private key.

- The private key resembles the password in Kerberos credentials, it confirms your identity.

- The file must be protected with a passphrase.

- Do not share this file with anyone. Do not send it by email.
- Do not share the passphrase.

What is a proxy?

- Temporary credential derived from an existing certificate.

- As an FNAL user, you can generate a VOMS proxy to run grid jobs and transfer data:
  - VOMS: Virtual Organization Membership Service
  - Your certificate(s) Distinguished Name(s) should be registered with your experiment.
  - A VOMS proxy contains information about your role in the experiment.
  - The VOMS proxy says what are you allowed to do within your experiment.

Authorization

- It is the process that determines whether an authenticated subject who has requested an action has the right to do so.

What are you allowed to do?

How a proxy is different from a certificate?

- It has a shorter lifetime than the certificate.
- Whoever has your proxy can act on your behalf, can act like you.
  - There is no security protection on your proxy.

What can you do with a proxy?

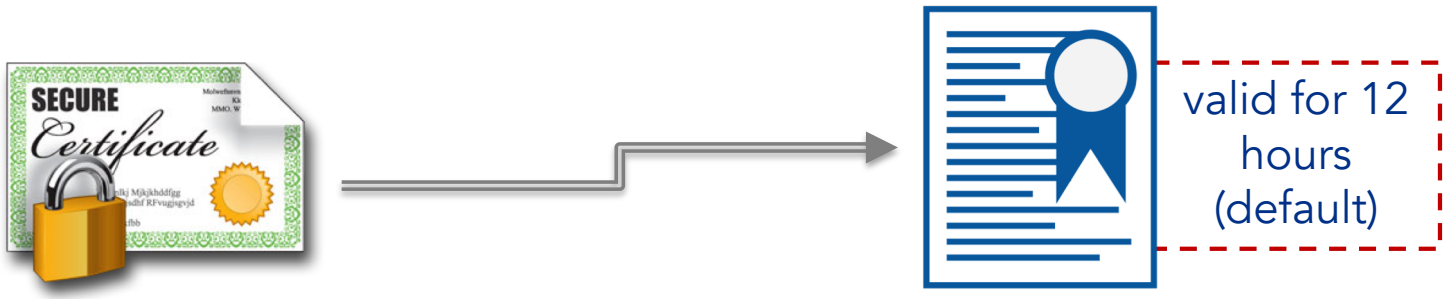
- You can submit jobs or initiate data transfers.
  - When you submit a job, you use the proxy to allow a computer process to run a task on your behalf.

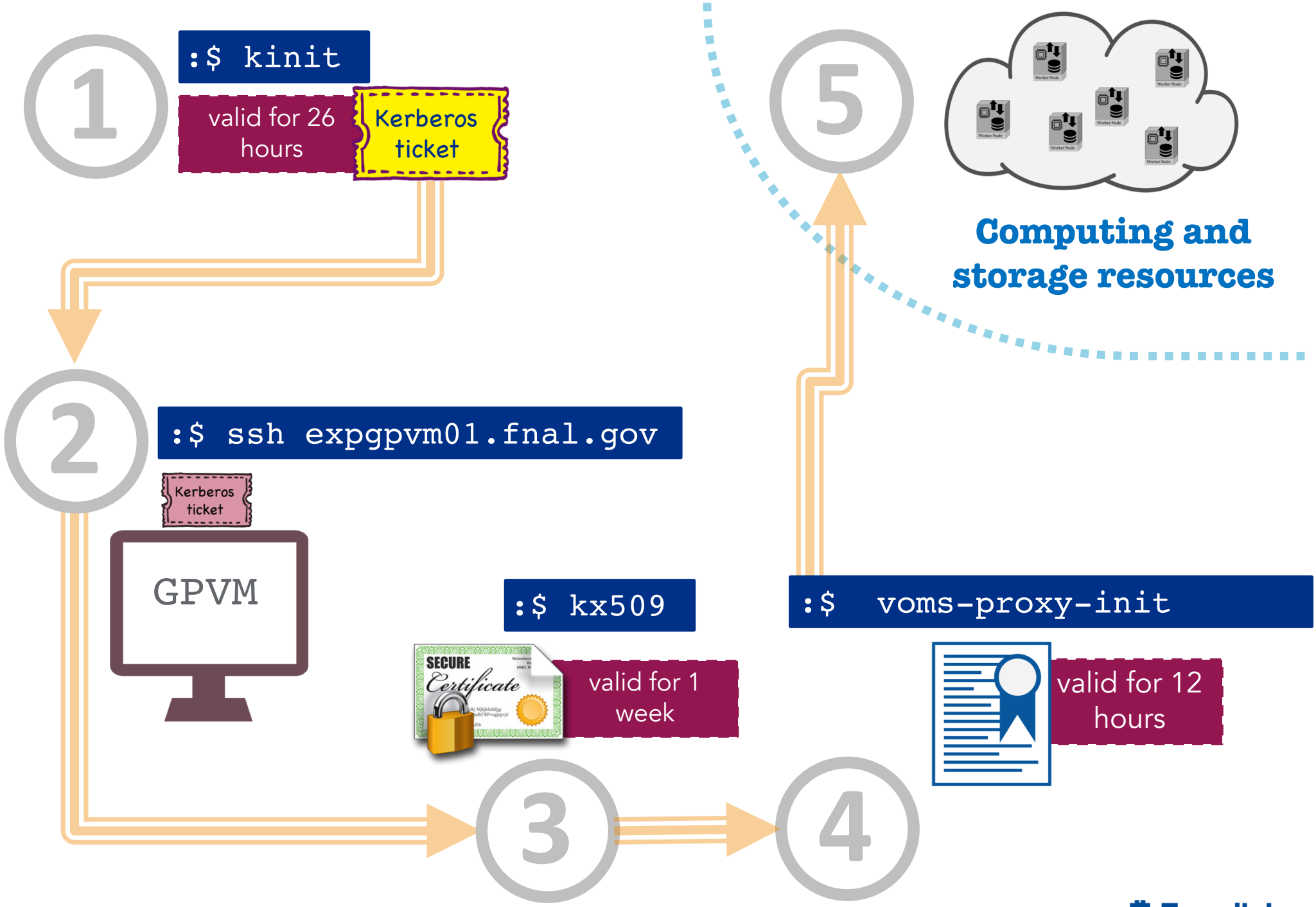
How do you get a proxy?

- By running the command voms-proxy-init .

```
:$ voms-proxy-init
```

creates an [X.509] proxy derived from your certificate with VOMS extensions: your role within your experiment according to the options passed to the command.




1
:$ kinit
valid for 26 hours
Kerberos ticket
2
:$ ssh expgpvm01.fnal.gov
Kerberos ticket
GPVM
:$ kx509
SECURE
Certificate
valid for 1 week
3
4
:$ voms-proxy-init
valid for 12 hours
5
Computing and storage resources

Summary

- Kerberos tickets, certificates and proxies are different ways of representing the identity of a subject.
- Depending on the resource or the service, you will use one or the other:
  - Kerberos tickets are used to SSH into your experiment interactive nodes.
  - Certificates are used to access some web services and to generate proxies.
  - Proxies are used to submit jobs to the grid and to handle scientific data.

Questions?